



Job Aid: Directory Application

Issue 1.1
August 26, 2010

Purpose

This job aid provides instructions for administering the Directory Application in the Avaya Aura™ Communication Manager 6.0 template.

Revisions

Issue 1.0	baseline version
Issue 1.1	added details for the CM 5.2 directory application

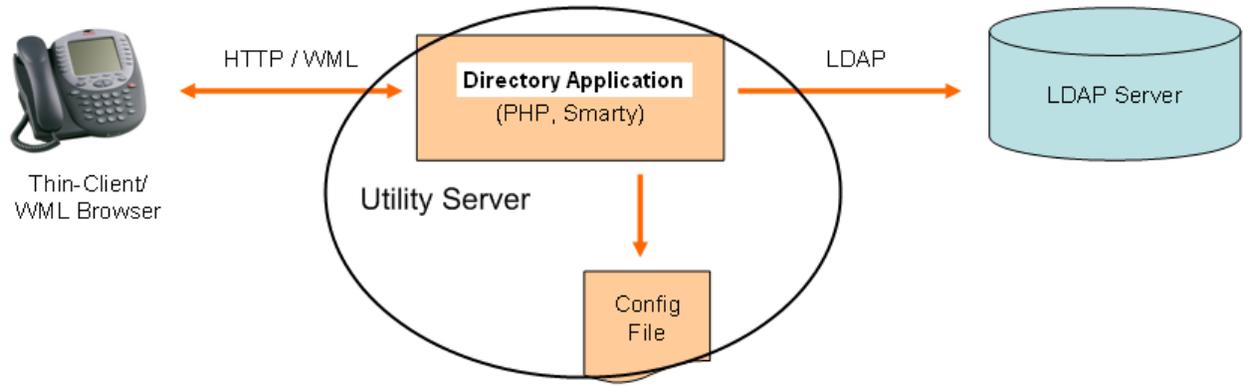
Audience

This document provides information for data and voice administrators who are responsible for managing the Communication Manager and the Utility Server in the Avaya Aura™ Communication Manager 6.0 template. Using the directory application requires knowledge of your dial plan and installed LDAP compliant database/schema.

Overview

The Avaya 4600 and 9600 Series IP Telephones feature an embedded Web Browser, allowing them to become application-enabled appliances instead of just phones. This allows developers to design Web-based enterprise applications that are accessible through the IP phones. One of these applications is the Directory Application; previously know as the Thin Client Directory Application. The Directory Application enables you to search an LDAP compliant database using the browser on your compatible 46xx and 96xx phones. You can use the Directory Application administration web pages to configure the Directory Application and customize the user search experience.

The Avaya Directory Application was introduced in Communication Manager 5.2 and is on the Communication Manager Servers: [“S8800, S8300D, S8500C, S8510, S8720 and S8730](#). This feature moved to the Utility Server in CM 6.0. This job aid is primarily aimed at CM 6.0 but it can be used for CM 5.2. Features not appearing in CM 5.2 are marked with “CM 6.0”



Accessing the Directory Application

- 1) Login to the Avaya Aura™ System Platform Web Console
- 2) On the Virtual Machine Management screen click on the Utility Server wrench (Manage Virtual Machine)
- 3) Login to the Avaya Aura™ System Platform Utility Server with the **admin** login
- 4) On the Avaya Aura™ Utility Server Administration screen click Administration and select Directory Application

Communication Manager 5.2.x

- 1) Login to the CM System Management Interface (SMI) Web Interface
- 2) Select “Directory Administration under the Administration menu item

Note: If you do not see the “Directory Administration” menu item on a supported CM 5.2 server (S8800, S8300D, S8500C, S8510, S8720 and S8730), it indicates that the “Web Access Mask” is configured incorrectly and this is preventing access to the directory application for this login. Try another login or change the profile for this login to allow access to the directory application.

You are now at the Directory Application Administration and will see the following screen.

The screenshot shows the Avaya Aura™ Utility Server Web Console interface. At the top left is the AVAYA logo. At the top right is the text "Avaya Aura™ Utility Server Web Console". Below the logo is a navigation bar with "Help" and "Log Off" on the left, and "Administration" and "Utilities" on the right. Below the navigation bar is a breadcrumb trail "Administration / Directory Application" and "This Server: utility". The main content area is titled "Directory Application Administration" and contains the following text: "The Directory Service application enables you to search an LDAP database using browsers on your compatible 96xx and 46xx phones. You can use these web pages to configure the Directory Service application to connect to an LDAP databas and to customize the user search experience." Below this text are three sections: "General Settings" (Administer general settings, LDAP connection settings, Search settings, Detail settings and LDAP Filter settings for the Directory Service application.), "Traslation Language Settings" (Customize the Translation Language web page of the Directory Service application to enable users to customize the language text strings.), and "External Numbers" (List, Add, Edit and Delete external numbers.).

Figure 1 Directory Application Administration

Prerequisites

Before you can administer the Directory Application, you will need to know the following:

- LDAP server IP address
- LDAP server port
- LDAP user id and password
- LDAP attributes
- Utility Server IP address

Quick Setup

To configure the Directory Application:

1. Select the directory number (1-250) that you wish to administer (CM 6.0)
2. Specify the LDAP connection settings in the **General Settings** section.
3. Click **Test Connection** to ensure that the Directory Application is connecting to the LDAP database.
4. Enable the Directory Application for HTTP or HTTPS traffic.
5. (Optional) Use the **Search Screen Settings** section to customize the Search screen on the phone browser.
6. (Optional) Use and the **Details Screen Settings** section to customize the **Details** screen on the phone browser.
7. (Optional) Use and the **LDAP Filter Settings** section to restrict the results based on the filters used.
8. Set the HTTP (or HTTPS) to point to the Utility Server via DHCP or in the 46xxsettings.txt file

Directory Number (CM 6.0)

Help Log Off Administration Utilities

Administration / Directory Application

Home
General Settings
Translation Language
External Numbers

Directory Number 185

General Administration

LDAP Administration

Search Screen Settings

Detail Screen Settings

Ldap Filter Settings

Save Test Connection Help

The Directory Application supports up to 250 directory instances. Each instance (Directory Number) can be administered uniquely. Use the Directory Number drop down list box to select the directory instance (1-250) you wish to administer.

Each directory instance may be considered as a stand alone Directory Application as all the administration is unique to each directory instance. The directory instances can be used to support tenant partitions, a multi-lingual environment, multiple LDAP databases, etc.

Note ► You may click on any title bar to expand that section.

General Administration

Application Title: Title displayed on the Browser bar.
Enter any Unicode text string up to 25 characters

HTTP: accept requests from phone WML browser over the unsecured HTTP connection

HTTPS: indicates that Directory Application will accept requests from the Avaya phone WML browser over the secured SSL based HTTPS connection.

General Administration	
Application Title	<input type="text" value="Directory Application"/>
HTTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTPS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Select a language file	<input type="text" value="English"/>
Select language for your translation	<input type="text" value="English"/>

Select a language file: (CM 6.0) Initially populated with English and 11 language folders: lang1, lang2 ... lang11. You can assign any language from the “Select language for your translation” to a language file. Once a language file is assigned a translation, the language name replaces the default file name (langX were X = 1-11). There is no provision to change a language file name so assign the translations carefully.

Select language for your translation: (CM 6.0) List of languages. If a language folder (langX) is selected (Select a language file), the language selected here will be placed in the language folder. If a language was selected in “Select a language file”, the language selected here must match that language.

Note ► Only the Avaya 9600SIP and the 96xx H.323 release 3.0 and greater support the HTTPS protocol.

After completing this section, click the Save button at bottom of page.

Language Assignment Example (CM 6.0)

This example assigns Japanese to language file lang10.

Select a language file

Select language for your translation



In the “**Select a language file**” drop down list box, select lang10

Select a language file

Select language for your translation

LDAP Administration

Host Name



In the “**Select language for your translation**”, select Japanese

General and ldap settings have been saved successfully.

Click the Save button at the bottom of page.

Directory Number

16

General Administration

Application Title

Directory Application

HTTP

Enable Disable

HTTPS

Enable Disable

Select a language file

Japanese

Select language for your translation

Japanese

Select a language file

Select language for your translation

LDAP Administration

Host Name

Port



The next time you click on “**Select a language file**”, Japanese has replaced the file name lang10.

This indicates that the file lang10 has been assigned a language and is no longer available for future assignment

LDAP Administration

LDAP Administration	
Host Name	<input type="text" value="135.27.153.201"/>
Port	<input type="text" value="389"/>
Base DN (Search Root)	<input type="text" value="o=avaya.com"/>
Base DN (External Search Root)	<input type="text" value="ou=external,o=avaya.com"/>
Max number of hits	<input type="text" value="96"/>
User Id (Optional)	<input type="text" value="cn=Manager,o=avaya.com"/>
Password (Optional)	<input type="password" value="••••"/>
Search Time	<input type="text" value="10"/> <input type="button" value="v"/>
Secure Connection (TLS support)	<input type="radio"/> On <input checked="" type="radio"/> Off

Host Name: The IP address of your LDAP server.

Port: The Port used of your LDAP server. Default = 389

Base DN: The starting point in the directory to conduct the search. All searches begin at or below the Base DN, depending on the scope, and move down the tree. An example of a Base DN is: ou=People,dc=example,dc=com.

The Test Connection (bottom of page) does not verify this field. If this value is incorrect, a user search will fail.

Base DN (External Search Root): The starting point in the directory to conduct the search for *external numbers*. Use the External Numbers administration screen to add, change and delete LDAP entries for entries outside of your corporate environment. The Test Connection does not verify this field. If this value is incorrect, a user search will fail.

Max number of hits: The maximum number of entries sent to a phone in response to a search. The search is stopped when the maximum number is reached. To decrease network traffic you should consider lowering this value. For most environments, it is recommended you stay with the default value of 96 as a higher number can degrade the network performance.

User ID (optional): It is not required if anonymous binding is used. Otherwise, this is the user id on the external LDAP server permitted to search the LDAP directory within the defined search base. If a user ID is specified, you must also provide the password for this user id.

Password (optional): This is the password for the user id. This is left blank if no user ID is specified.

Search Time: Sets the maximum length of time in seconds that the directory server should spend processing any search request. The default is set to 10 seconds. Note that the LDAP directory server may enforce a lower time limit than the one requested by the Directory Application.

Secure Connection (TLS support): This option requires a certificate. Refer to the TLS Configuration later in this job aid for more details.

After completing this section, click the Save button at bottom of page. Next click **Test Connection** at the bottom of the page to ensure that the Directory Application can connect to the LDAP server using the connection parameters you have specified. If the values you entered for Host Name, Port and User Id (optional) are correct, you will see a “Connection Successful” message at the top of the page.

Search Screen Settings

You can define up to 6 attributes to search for. You may also assign a label to the attribute. These attributes & labels appear on the phone search User Interface.

Search Screen Settings		
#	Search Attribute	Associated Label (Max 20 characters)
1	cn	Surname
2	telephoneNumber	Phone
3	givenName	GivenName
4	c	Country
5	(other)	Company
	tconame	
6	(other)	Dept
	dptName	
7	Min chars in the Search String	4

Search attribute 1: This must be cn (Common Name) or cn;lang-en. The latter is used with multi-lingual databases where cn is populated with a name not using the Latin writing script and cn;lang-en is populated with the Romanized transliteration of the name in cn. If you don't have a multi-lingual LDAP use the cn attribute.

Search attribute 2: This entry must be a telephone number as the Avaya phones always expect the 2nd entry to be a phone number as this entry is put into the telephone entry of the phone's speed dial when the user selects "AddToSD"

Search attributes 3 - 6: The drop down list box provides many commonly used LDAP attributes. If your database uses an attribute name, not in the drop down list box, you can select other and then enter the attribute name in the pop up field.

Min Chars in the Search String: (CM 6.0) The minimum number of characters (1 – 9) required for user entered Search Strings. The directory application denies any search when the search string contains less than the minimum number of characters required.

5381234		10:15 3/24	
Browser		Phone Directory	
[Surname]			
[Phone]			
[GivenName]			
[Country]			
[Company]			
[Dept]			
Search	Clear	Help	More

This phone screen illustrates the relationship between the administration of the Search Screen Settings and the search screen on the user's 96xx phone.

The current WML screen is cached, so if you navigate among cards in the same deck, they are displayed from the cache. Changes made to this screen may take up to 5 minutes before the user sees the new screen. If you want to load a new version of search screen from the server, press the Refresh softkey (the icon is two horizontal arrows pointing in opposite directions).

After completing this section, click the Save button at bottom of page.

Detail Screen Settings

You can define up to 6 attributes for display on the user's Detail Screen. You may also assign a label to each attribute.

Detail Screen Settings		
#	Detail Attribute	Associated Label (Max 8 characters)
1	displayName	Name
2	telephoneNumber	Phone
3	(other) jobfun	Function
4	(other) dptname	Dept
5	(other) sname	Manager
6	mail	Email

Detail attribute 1: This must be cn (Common Name), displayName or cn;lang-en. The latter is used with multi-lingual databases where cn is populated with a name not using the Latin writing script and cn;lang-en is populated with the Romanized transliteration of the cn value.

Detail attribute 2: Avaya phones always expect the 2nd entry to be a phone number as this entry is put into the telephone entry of the phone's speed dial when the user selects "AddToSD"

Detail attributes 3 - 6: The drop down list box provides many commonly used LDAP attributes. If your database uses an attribute name, not in the drop down list box, you can select other and then enter the attribute name in the pop up field.

5381234	10:16 3/24
Browser Contact Details	
Name: Young, Neil	
Phone: +13035381234	
Function: System Engineer	
Dept: Sales	
Manager: Gabriel, Peter	
Email: nyoung@avaya.com	
Search	AddToSD
Return	More

This phone screen capture illustrates the relationship between the administration of the Detail Screen Settings and the Detail screen on the user's 96xx phone.

The current WML screen is cached, so if you navigate among cards in the same deck, they are displayed from the cache. Changes made to this screen may take up to 5 minutes before the user sees the new screen. If you want to load a new version of search screen from the server, press the Refresh softkey (the icon is two horizontal arrows pointing in opposite directions).

After completing this section, click the Save button at bottom of page.

LDAP Filter Settings (CM 6.0)

This section is used to restrict the search results. The filter attribute can be any attribute used in your LDAP compliant database. The Filter Text is a value assigned to that attribute.

Ldap Filter Settings		
#	Filter Attribute	Filter Text (Max 20 characters)
1	dptBusinessGroupName	Services
2	region	NAR
3	(none)	
4	(none)	
5	(none)	
6	(none)	

Use the drop down list boxes to select an LDAP attribute. Use the Filter Text box to enter a string used for the each attribute. The LDAP search will only send results for entries that contain the string in each attribute

With the settings to the right, all searches only return results for entries that the value in dptBusinessGroupName begin with Services AND the value in region begins with NAR.

Note ► The wildcard is appended to the end of the Filter Text string.

After completing this section, click the Save button at bottom of page.

Translation Language (CM 6.0)

This screen is accessed via the Translation Language link (left pane) under the Administration/Directory Administration menu.

Language Translation Settings

Customize the Translation Language screen of the Directory Application.

Language Translation is selected for **Japanese**

#	Text String	Translation
1	Clear	クリア
2	Help	ヘルプ
3	Search	検索
4	+Contact	登録
5	Detail	詳細
6	Call	発信
7	AddToSD	登録
8	Return	戻る
9	Done	完了
10	Retry	再検索

The directory application comes with 13 built-in translations. This section contains all the strings used on the phone screens: button labels, menu labels, help and error messages.

You can enter or change the translation for any string. The language being modified on this screen is determined by the General Settings field “Select language for your translation”

After completing this section, click the Save button at bottom of page.

External Numbers

This screen is accessed via the External Numbers link (left pane) under Administration/Directory Administration.

External Numbers Administration

List, Add, Edit and Delete numbers.

#	Native Name	Name	Phone Number	Email
<input type="checkbox"/>	Gyalog, László		8318	Igyalog
<input type="checkbox"/>	Btiö, ganesh	ganesh	2805	
<input type="checkbox"/>	Ganesh, machkure	mak1		
<input type="checkbox"/>	Ganesh,Mak	Mak		
<input type="checkbox"/>	Ganesh,,,, Machkure	Makie	456231	
<input type="checkbox"/>	Ganesh-IP		48999	
<input type="checkbox"/>	ganesh,machkure	mak	456123	
<input type="checkbox"/>	Ganesh Machkure	Ganesh Machkure	30412805	
<input type="checkbox"/>	Ganesh \tMachkure1	Ganesh\t Machkure1	30412805	

Page 4 of 4

This section allows you to List, Add, Edit and Delete numbers pertaining to LDAP records that are not populated with Communication Manager station name and number. To ensure that you can modify the LDAP database using the **Manage External Numbers** screen, you must give write access to the specified user for the database.

Additionally, the General Settings field “Base DN (External Search Root)” must point to the distinguished name used for external numbers. If the value used for this field is incorrect, this screen will not be available.

TLS Configuration

The Directory Application can connect to an LDAP server on TCP or TLS. If you choose to select TLS as the connection type, the below additional configuration must be done using the `esdtlscert` bash command line tool. You should only enable TLS after verifying that a TCP implementation works successfully (user search works from phone). For investigation of problems, you must use a non-TLS connection in order to analyze traffic between the directory application and your LDAP server.

- Install a Certificate Authority (CA) certificate file (Required)
- Enable/Disable Client certificates and Client Side Authentication

Note: For all the configurations, you must log into Utility Server bash interface command line with `SUSER` permissions to run the `esdtlscert` command.

DISPLAY CONFIGURATION

You can use the `esdtlscert` to see the current TLS configuration for the Directory Application.

To see the current configuration:

1. Log into the Utility Server bash interface command line.
2. Type `esdtlscert` command to display the current information.

INSTALL CERTIFICATE AUTHORITY (CA) CERTIFICATE FILE

For TLS connection to work, at least a CA certificate is required so that the Directory Application can recognize the server certificates.

To install a CA certificate:

1. Log into the Utility Server bash interface command line.
2. Type `esdtlscert --cacert filename` to install the file containing certificates for all of the Certificate Authorities the Directory Application will recognize.

By default, the configuration is set to perform very strict checks on the server certificates.

To change the level of checks:

1. Log into the Utility Server bash interface command line.
2. Type `esdtlscert --certcheck level`, where The `<level>` can be specified as one of the following keywords:
 - **never:** The client will not request or check any server certificate.

- **allow**: The server certificate is requested. If no certificate is provided, the session proceeds normally. If a bad certificate is provided, it will be ignored and the session proceeds normally.
- **try**: The server certificate is requested. If no certificate is provided, the session proceeds normally. If a bad certificate is provided, the session is immediately terminated.
- **demand**: The server certificate is requested. If you do not provide any certificate, or provide a bad certificate, the session is immediately terminated. This is the default setting and the default level.

ENABLE CLIENT SIDE AUTHENTICATION

You can optionally enable Client Side Authentication so that the LDAP server can authenticate the Directory Application. Perform the following to enable it.

- Install a client certificate.
- Install a private keys file that matches the client certificate.
- Specify acceptable cipher suites and preference order.
- Enable Client Side Authentication.

To install a Client certificate:

1. Log into the Utility Server bash interface command line.
2. Type **esdtlscert --cert filename** command to install the file that contains the Client certificate.

To install private keys:

1. Log into the Utility Server bash interface command line.
2. Type **esdtlscert --key filename** to install the file that contains the private keys that match the client certificate.

To specify the cipher suites:

1. Log into the Utility Server bash interface command line.
2. Type **esdtlscert --cipher cipher_suite**, where the **cipher_suite** should be a cipher specification for OpenSSL, for example, HIGH:MEDIUM:+SSLv2.

To enable the client side authentication:

1. Log into the Utility Server bash interface command line.
2. Type **esdtlscert --clientcert enable** to enable client side authentication.

Configuring phones to use the Directory Application

The 46xxsettings.txt file is used to specify certain system parameters for the 4600 and 9600 series phones. The WMLHOME parameter will either point directly or indirectly to the Directory Application. The Utility Server comes with a 46xxsettings.txt file and the WMLHOME parameter is automatically setup to point to a landing page which includes 3 WML applications: Directory Application, User entered URL, Message Application. For an in-depth analysis on how this is implemented, refer to the Detailed Information section later in this Job Aid.

Phone Groups

If you are using more than one directory instance, you will want to put your phones into Groups. You may assign an IP Phone to a Group on the station form (Figure 2) or in the phone firmware (craft mode). The phone GROUP ID determines the directory application. Thus a phone with an IP Phone Group ID = 230, will get directory application instance 230. The Utility Server will automatically direct a phone to the correct directory application instance based on the phone's GROUP ID.

```
add station next                                     Page 3 of 5
                                                    STATION
    Conf/Trans on Primary Appearance? n
    Bridged Appearance Origination Restriction? n

    Call Appearance Display Format: disp-param-default
    IP Phone Group ID: 230

    ENHANCED CALL FORWARDING
    Forwarded Destination                               Active
    Unconditional For Internal Calls To: _____ n
    External Calls To: _____ n
    Busy For Internal Calls To: _____ n
    External Calls To: _____ n
    No Reply For Internal Calls To: _____ n
    External Calls To: _____ n

    SAC/CF Override: n
```

Figure 2 IP Phone Group ID

Calling external numbers

Entries returned from a search may have an internal or an external phone number. The user wants the capability to press the call button and dial a number regardless if that number is internal or external. While this is outside the scope of this job aid, some details on Communication Manager and phone administration are included to help you with automatic call out.

Depending on how telephone numbers are stored in your database, you may want to setup ARS digit analysis table on the Communication Manager server. Refer to the Call Type Digit Analysis example and the AAR and ARS Digit Analysis Table in the Administrator Guide for Avaya Communication Manager.

You may also provide the ability to call external numbers via the ENHANCED LOCAL DIALING (ELD) RULES in the phone's 46xxsettings.txt file. Note, that ELD does not apply to numbers in the user's contact list. For more details on setting up ELD, refer to the "IP Telephones LAN Administrator Guide".

Additional Details

If the Communication Manager has been administered for Call Type Digit Analysis, it and the telephone will exchange that information when the telephone registers, and the telephone will assume it can ignore the settings file parameters (i.e. phone no longer uses ELD), and count on Communication Manager to do Call Type Digit Analysis on any call dialed from the Call Log or the Browser. The telephone passes such numbers to Communication Manager via smart enbloc, which is the mechanism that triggers Communication Manager's use of Call Type Digit Analysis.

Note the telephone assumes any number in the Contacts application is dialable as is, and so uses "dumb" enbloc dialing to pass those digits to Communication Manager. In addition, manual dialing is done in overlap sending, so Call Type Digit Analysis is not invoked. Finally, for features where the telephone is not really dialing, but instead invoking a feature (e.g. "Call Displayed Number", aka call-disp for the Integrated Directory feature), then of course all the phone sends is a button press, and it's up to Communication Manager to dial the call as it sees fit.

If Communication Manager has not been administered for Call Type Digit Analysis (including versions of Communication Manager that do not support Call Type Digit Analysis), the telephone does care about the settings file, and the suite of parameters that comprise the Enhanced Local Dialing (ELD) feature.

The following is a brief overview of ELD

:

- 1) ELD only applies to calls made from the Incoming Call Log (either Answered or Missed) or the Browser. Calls made manually, or from Contacts, or from Outgoing Call Logs, or from Communication Manager -based features (e.g. call-disp) are not subject to ELD.
- 2) Assume the phone number stored on the phone is X (where X can be of any length up to 30 characters). If the first character of X is a "+", (e.g. from the Directory Application look-up), the phone assumes the call is to be handled as an international call, and a different leg of the algorithm is handled. Otherwise, the telephone assumes the call to be handled is not international.
- 3) After removing any non-dialable characters from X (e.g. formatting characters like parentheses, dashes, etc.), set L to the length of X in characters (so if X was "1234", L=4).
- 4) Compare L to settings file parameter PHNDPLENGTH (the "DP" refers to "dial plan"). If L is less than or equal to PHNDPLENGTH, X is assumed to be a number that is part of the local dial plan (e.g. a 5-digit phone number is probably an internal call if ACP has a 5-digit dialing plan). In this case, the phone dials X without any changes, and we're done.
- 5) Assuming L is strictly greater than L, X is assumed to be a local or a national number, not an on-network number. We compare L to settings file parameter PHLDPLENGTH (the "LD" refers to "long distance"). If L is equal to PHLDPLENGTH, X is assumed to be a national number, so the

phone dials PHNOL (for the outside line) + PHNLD (the long distance access code) + X, and we're done.

6) Assuming L is not equal to PHNLDLENGTH, X is assumed to be a number that only needs access to an outside line, so we dial PHNOL + X, and we're done.

Detailed Information

This section is provided for administrators that want a more detailed explanation on how the Utility Server uses a Phone Group ID to point a phone to the appropriate WML applications, including the Directory Application. The files mentioned in this section should not be manually edited or removed as the Utility Server will automatically populate them with data.

In the Utility Server 46xxsettings.txt file is the line "GET ESD_Landing.txt. The ESD_Landing.txt file is loaded into the 46xxsettingx.txt and has all the logic to direct a phone to the landing (home) page based on the phone's group ID.

The ESD_Landing.txt partial contents are shown below. Note that the IP address 135.64.158.33 is for a Utility Server installed in the Avaya network. The network plug-in will populate your Utility Server IP address in this file at installation time

```
# ESD with the capability of 250 different WML Landing Pages
# based on the phones GROUP parameter.
# By default, the phone will use landing.wml
#
IF $GROUP SEQ 1 GOTO TENANT_1
IF $GROUP SEQ 2 GOTO TENANT_2
IF $GROUP SEQ 3 GOTO TENANT_3
    < lines deleted >
IF $GROUP SEQ 248 GOTO TENANT_248
IF $GROUP SEQ 249 GOTO TENANT_249
## Do not handle anything other than 1 through to 250
# The default for an unknown group number is the standard page
SET WMLHOME http://135.64.158.33/landing.wml
GOTO EXIT

# TENANT_1
SET WMLHOME http://135.64.158.33/landing_1.wml
GOTO EXIT
# TENANT_2
SET WMLHOME http://135.64.158.33/landing_2.wml
GOTO EXIT
    < lines deleted >
# TENANT_248
SET WMLHOME http://135.64.158.33/landing_248.wml
GOTO EXIT
# TENANT_249
SET WMLHOME http://135.64.158.33/landing_249.wml
GOTO EXIT
# TENANT_250
SET WMLHOME http://135.64.158.33/landing_250.wml
GOTO EXIT
## THIS REALLY IS THE END
# EXIT
```

There are 250 landing pages, named landing_1.wml, landing_2.wml... landing_249.wml, landing_250.wml. The contents of all these files are the same except for the reference to the directory client. For example: landing_1.wml points to directoryclient1 (see code below), landing_2.wml points to directoryclient2, etc. There is a directory client folder for each directory instance (1-250)

landing_1.wml

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
"http://www.wapforum.org/DTD/wml13.dtd">
<wml>
<card id="menu" title="Menu">
  <p><a href="directoryclient1/search.php">Directory Client</a></p>
  <p><a href="web_addr.wml">Enter a Web Address (WML)</a></p>
  <p><a href="message.wml">Message Board</a></p>
</card>
</wml>
```

Failure Messages sent to phone

For more details on LDAP error conditions, refer to <https://www.opends.org/wiki/page/DefinitionResultCode>

Cause of Search Failure	LDAP Result Code(s)	Failure Message	Things to Check
The URL used for the search screen could not be found	N/A	404: Not found	That the HTTP server on the Utility Server is running. If the HTTP server is running, restart it. Also, check the URL used for the WMLHOME is correct. If you are using the AvayaMenuAdmin.txt for the Directory Application, check that the URL listed for the AMDATA entry is correct
Operations/Protocol error	1, 2	An unknown problem has occurred	that the TDN is pointing to the correct DN in your LDAP compliant database
Server-generated time-out	3	Server timed out	that the directory server is running
Authentication not accepted	7, 8, 48, 49, 50, 53	Authentication error	Login credentials are correct
Telephone Number not recognized	16, 17	Telephone Number not recognized	That you are using the correct attribute name
Object not found	32	No results found	

Server responds with “null” as data	N/A	No results found	
Server not available	51, 52	Server not available	That you have network connectivity to the ldap server and that it is running
Other, unspecified	80	An unknown problem has occurred	
The directory server does not respond at all within an administrable amount of seconds (default is 10 seconds)	N/A	Connection Failure	
When Directory Application receives a request for a Search screen, it will send a Search screen in response only if the minimum administrative information has been supplied. Otherwise, a Trouble Screen will be sent to the phone.	N/A	Insufficient Administrative Information	
When Directory Application receives a request for a search from a phone, it will initiate a connection to the directory database server and, if successful, it will format and send a query to the database server based on the input received from the endpoint. If the input received from the endpoint is null, a Screen will be sent to the phone.	N/A	Insufficient Query Information	
If a connection to the database server cannot be established, or if the connection fails before a response is received, a Trouble Screen will be sent to the phone.	N/A	Connection Failure	

Directory Application receives a successful response from the database server, it sends a Successful Result screen to the endpoint. If no matching database entries are returned, it sends a No Match Result screen to the endpoint. If an error is returned by the database, a Trouble screen is sent to the phone.	N/A	No results found	
--	-----	------------------	--